

The Gaussian integers

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

Recall: an element a of the commutative ring R is **irreducible** provided a is not a unit and $a = bc$ implies that b or c is a unit.

2 is not irreducible in $\mathbb{Z}[i]$ because $(1 + i)(1 - i) = 2$.

Norm

$$N(a + bi) = a^2 + b^2.$$

- $N(z) = 0$ if and only if $z = 0$.
- If z is a Gaussian integer, then $N(z)$ is an integer, and $N(z) = 1$ if and only if z is a unit
- $N(z_1 z_2) = N(z_1)N(z_2)$

If $N(z)$ is a prime, then z is an irreducible in \mathbb{Z} .

Why? $xy = z \Rightarrow N(x)N(y) = N(z) \Rightarrow N(x) \text{ or } N(y) = 1 \Rightarrow x \text{ or } y$ is a unit.

Example: $1 + 2i$ is an irreducible in \mathbb{Z} .

We claim that 3 is irreducible in the complex numbers.

Suppose that $3 = ab$, where $a, b, \in \mathbb{Z}[i]$.

Then $9 = N(3) = N(a)N(b)$. If $N(a) = 1$ or $N(b) = 1$ we're done.

Otherwise $N(a) = 3$. This means there are integers x and y with $x^2 + y^2 = 3$ —which is impossible.

So either a or b is a unit.

Express $165 + 490i$ as a product of irreducibles in $\mathbb{Z}[i]$.

$$165 + 490i = 5(35 + 98i) = 5 * 7(5 + 14i).$$

$5 = (1 + 2i)(1 - 2i)$ So:

$$165 + 490i = (1 + 2i)(1 - 2i) * 7 * (5 + 14i)$$

$1 + 2i$ and $1 - 2i$ are irreducible, since their norms are a prime.

7 is irreducible, since $a^2 + b^2 = 7$ has not integer solutions.

What about $5 + 14i$; This has norm $221 = 13 * 17$. So if not irreducible, we are looking for $x = a + bi$ and $y = c + di$ with $xy = 5 + 14i$ and $a^2 + b^2 = 13$ and $c^2 + d^2 = 17$.

This gives $a, b \in \{\pm 2, \pm 3\}$ and $c, d \in \{\pm 1, \pm 4\}$

$x = 2 + 3i$ and $y = 1 + 4i$ works; and x and y are irreducible.

So $165 + 490i = 7(1 + 2i)(1 - 2i)(2 + 3i)(1 + 4i)$.

Fundamental Theorem for the Gaussian Integers

Every Gaussian integer is either 0, a unit, irreducible or the products of irreducibles.

Why?

If not irreducible nor unit nor 0, then $a = bc$ for some bc with neither b nor c a unit.

So $N(a) = N(b)N(c)$ and $N(b) < N(a)$ and $N(c) < N(a)$.

So we can "factor" b and c to get factorization of a .

Division Algorithm for the Gaussian integers

Let a and b be Gaussian integers, with $b \neq 0$. Then there exist q and r such that $a = bq + r$ where $N(r) < N(b)$.

Algorithm: Compute a/b in the complexes, say $a/b = u + iv$. Now let u' be the closest integer to u , and v' be the closest integer to v .

Set $q = u' + iv'$, $r = a - bq$.

Why does this work? $a - bq = b(a/b - q)$. So $N(r) = N(b)N(a/b - q)$ and $N(a/b - q) = N(u - u' + i(v - v')) = (u - u')^2 + (v - v')^2 \leq (.5)^2 + (.5)^2 < 1$.

So $N(r) < N(b)$.

Example:

Find the quotient and remainder when $3 + 5i$ is divided by $1 + 2i$ in $\mathbb{Z}[i]$.

$$\frac{3+5i}{1+2i} = \frac{(3+5i)(1-2i)}{5} = \frac{13-i}{5} = 13/5 - (1/5)i.$$

So $q = 2 + 0i$ and $r = 3 + 5i - 2(1 - 2i) = 1 + i$.

Check: $3 + 5i = 2(1 + 2i) + (1 + i)$ and
 $N(1 + i) = 2 < 5 = N(1 + 2i)$.

Note: Quotient and remainder are not unique!

Once we have the Division Algorithm, we can mimic Euclid's proof to get:

If a is irreducible in $\mathbb{Z}[i]$ and $a|bc$, then $a|b$ or $a|c$.

Def'n In a domain, a is a prime if a is a nonzero, non-unit such that $a|bc \Rightarrow a|b$ or $a|c$.

Almost agrees with normal def'n in case of \mathbb{Z} . Get $\pm p$

Let's show there are no positive integer solutions to $x^2 + 1 = y^3$.

Suppose there were. Note $x^2 + 1 = (x + i)(x - i) = y^3$ in the Gaussian integers.

By Euclid's Lemma, both $x + i$ and $x - i$ divide y .

Thus $x^2 + 1$ divides y , say $(x^2 + 1)k = y$.

Substitution gives $x^2 + 1 = k^3(x^2 + 1)^3$.

so $(x^2 + 1)(k^3(x^2 + 1)^2 - 1) = 0$.

Integral domain implies $k^3(x^2 + 1) = 1$.

Taking norms implies that $x^2 + 1$ must be 1.

But then $x = 0$.

Now the integral domain $\mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{5}bi : a, b \in \mathbb{Z}\}$ behaves quite differently.

Still have a norm: $N(a + \sqrt{5}bi) = a^2 + 5b^2$; with the properties as before.

Units just ± 1 .

$6 = 2 \cdot 3$; 2 and 3 irreducible, since $a^2 + 5b^2 = 2$ and $c^2 + 5d^2 = 3$ has no integer solutions.

$6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$; and $1 + \sqrt{5}i$ and $1 - \sqrt{5}i$ are both irreducible. (Since their norms are 6).

In $\mathbb{Z}[\sqrt{-5}]$: there is not unique factorization!

So there is no division algorithm.

Euclid's Lemma fails!: 2 divides $6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$; but 2 does not divide either of the factors.